The Federal Communications Commission
Washington DC 20554

In the Matter of	)	
	)	
Implementation of the Child Safe Viewing Act;	)	**MB Docket No. 09-26**
Examination of Parental Control Technologies	)	
for Video or Audio Programming	)	
	)	
Notice of Inquiry	)	
	)	

Comments of Digimarc Corporation

Introduction

Digimarc Corporation ("Digimarc") is pleased to submit the following comments in response to the above-captioned Notice of Inquiry ("NOI"). Located in Beaverton, Oregon, Digimarc is an established innovator in digital watermarking technology. The company offers a wide range of technology solutions, including advanced blocking technologies, to provide consumers with more choice regarding when, where, and how they want to access, or not access, media content. Additionally, Digimarc develops solutions, licenses its intellectual property, and provides development services to business partners across a range of industries, including national security, marketing, and media and entertainment. Digimarc has an extensive intellectual property portfolio, with more than 490 U.S. and foreign patents, and more than 400 patents pending in digital watermarking, media identification and management, and related technologies. More information about Digimarc can be found on our website, www.digimarc.com.

For years, Digimarc has sought to provide a safe media and entertainment environment for children. We participated in the creation and deployment of the V-Chip in 2003 and worked closely with the Internet Content Rating Association ("ICRA") to encourage content providers to flag adult-related content. ICRA is now known as the FOSI, or Family Online Safety Institute. For more information regarding FOSI and Digimarc's early collaboration in this area, see http://www.fosi.org/projects/.

In addressing the questions raised by the Federal Communications Commission ("FCC") regarding parental control technologies, Digimarc recommends that the FCC focus on approaches to parental control where the data that enables such control is contained in the content itself. This can be accomplished using digital watermarking, a technology whereby a digital code is embedded in all forms of content, imperceptible to people but detectable by machines. This technology is widely and successfully deployed in a broad range of applications. *See Appendices A through C.*

Digimarc believes that digital watermarking of content is an effective, broad-based solution to enable parents to control the content to which their children have access across various distribution platforms. Digimarc has many years of experience with digital watermarking and makes this recommendation because it will provide great flexibility. It will ensure that advanced content blocking can be carried out across the numerous delivery platforms which are, and will be, used to view content that may be inappropriate for children.

Executive Summary

In the NOI, the FCC requested comments on advanced blocking technologies currently available or in development that are capable of operating across multiple platforms. Digimarc respectfully submits that the FCC focus on technologies that enable the content itself to be a permanent, intrinsic and declarative part of the advanced blocking solution in any and all distribution channels, both present and future.

Digital watermarking is an imperceptible content identification technology described in the next section of this comment letter; it is an alternative technology to the V-Chip that can be used to accomplish advanced content blocking while providing more flexibility for parental control and portability across media consumption platforms.[1] As described more fully below, the data carried in the digital watermark can be used to block virtually any form of content (i.e., images, audio, and video content) deemed to be inappropriate for children and can be used across multiple platforms on multiple devices that view and distribute such content in the home and on mobile devices. A digital watermark cannot be easily stripped out, and will stay with the content through subsequent manipulations, copying, and format conversions. Thus, digital watermarks provide parents, content owners and content distributors with an effective, streamlined advanced blocking technology. Many industries, including the media and entertainment industry, already use digital watermarking and recognize its value. The technology has been proven through wide deployment and is in use in billions of digitally watermarked objects and hundreds of millions of digital watermark readers. Accordingly, effective use of digital watermarking can prevent unauthorized access to copyrighted work and block children from viewing indecent or objectionable programming, benefiting both content providers and parents.

[1] Digital watermarks are easily detected after distribution, enabling all forms of media and many objects to be given a unique digital identity. Technologies for digital watermarking exist for digital images, sound recordings, and audiovisual material, such as television and motion pictures. The technical and commercial feasibility of digital watermarking has already been proven in all major media types, including video, audio, bank notes, printed materials and digital photography, with billions of digitally watermarked objects in distribution and hundreds of millions of readers in place to detect those digital watermarks.

Discussion

I. Digital Watermarking Technology

A digital watermark is a digital code that can be embedded in all forms of content, imperceptible to people but detectable by computers, networks, and other electronic devices. *See an example in Figure 1 on Page 11.* Conceptually, it is analogous to the traditional notion of a watermark on paper, in which a barely perceptible mark is applied during manufacture that establishes the origin of the paper on later inspection. Similarly, digital watermarks applied to digital content are persistent, staying with the content through manipulation, copying, and format conversions.

When a device reads digital watermarks, the watermark can trigger a rules-based response that allows the content to be either viewed or not viewed. Through the use of watermarks, companies can track usage, convey copyright ownership, and allow or block access to their content. These are common uses of digital watermarking today.

A digital watermark is a form of imperceptible data inserted into content and can be used effectively in this embodiment as a means for enabling parental control of content viewing by children. The "data" carried in the watermark can be semantic (i.e. carry meaning in its own right), simply be a reference number, or in some cases, both. For example, part of the watermark may be informative and declare the nature of the content (e.g. "Adult"), and in a different portion of the watermark, carry a reference number, such as 1234. The reference number may point to an online ratings database, such as the Motion Picture Rating System. Thus, when a device "reads" the watermark, it could trigger an automatic action, such as "Block," based on the information carried in the watermark, or it may block the content after cross referencing the content with the database in question. In such a case, content that may have been labeled "Adult" by the content owner may be labeled as "TV17" by the ratings database. In this instance, the content would be blocked only if the parent has set the parameters to block only "R" content rather than other delineations. Furthermore, if the device lost connection to the Internet, the fallback would be "Block," giving parents further peace of mind.

In recent years, digital watermarks have emerged as a broad-based, affordable, and scalable solution to protect and identify media and other content. Digital watermarking has been employed by many national governments and their central banks to deter the counterfeiting of currency on a global basis. Moreover, many prominent corporations have embraced and invested in watermarking technology. For example, The Nielsen Company uses digital watermarking to automate the television ratings system and authenticate broadcasts. As a result of their efforts, all televised broadcasts now use digital watermarks to track viewership among Nielsen Families (those families that opt-in for audience measurement). All major record labels (including Sony BMG, Universal Music Group and Warner Music) use digital watermarks to identify and track leaks of promotional pre-release music onto the Internet.

II. Digital Watermarking Is a Content-Persistent Technology That Is Compatible With Multiple Platforms

In the NOI, the FCC requested comments on advanced blocking technologies currently available or in development that are capable of operating across multiple platforms. Digimarc respectfully submits that digital watermarking is one of the *very few technologies, if not the only technology*, available that is capable of operating across multiple content types and multiple platforms while addressing all of the FCC requirements for achieving effective content blocking. This is because digital watermarks are *content-persistent*, rather than channel or device-specific. In other words, digital watermarks become part of the content and therefore are always part of the solution. *Rather than identifying a solution that can be developed around a particular distribution channel and hoping for solution portability, digital watermarking enables the content itself to become a permanent, intrinsic and declarative part of the advanced blocking solution in any and all distribution channels, both present and future.* In contrast, the V-chip was a solution developed exclusively for TV distribution. In today's digital world, solutions need not be limited to a single distribution channel. Digimarc respectfully submits that the use of digital watermarking is a practical and responsible approach in achieving an effective and extensible advanced blocking solution on many levels across current and future distribution channels.

The importance of employing a technology that is content-persistent cannot be overstated. With the ubiquity of broadband across the United States and the proliferation of different content formats in multi-functional devices in homes and among mobile users, an effective advanced blocking solution *must* be content-persistent rather than hardware, software, or distribution-specific. By making the content itself part of the solution, regardless how the content is acquired or consumed, parents are able to control access to the material. Additionally, because it is not tied to a specific hardware or software component, digital watermarking can be integrated into future digital distribution paths and devices that have yet to be developed.

III. Digital Watermarking Can Block Content on Televisions, Through Cable and Satellite Transmissions, on Wireless Devices, on Non-Network Devices, and Available Over the Internet

As demonstrated in the following sections A through E, digital watermarking provides a substantially similar implementation approach across different reader deployments. *See the example in Figure 2 on Page 16.* Irrespective of the of the content transmission means and detection ecosystem involved, the watermark is deployed in the content in the same manner. In each instance, the digital watermark can be designed to carry both semantic (or informative) information and a reference number. The informative information includes the highest level "label" that the industry cooperatively agrees on (e.g. "Mature Audience") but is open to further interpretation, and ultimately decided by the parent. The reference number points to an online database in which the "connected" device can further classify the content based on its distribution channel (e.g. TV Parental

Guidelines system developed by Congress, the television industry and the FCC, and that went into effect by January 1, 1997).

In each scenario that follows, if content owners proactively apply a watermark during production *or* distribution, the content can be blocked. Also note that these are all illustrative examples of how the technology can be implemented. The actual implementations would require cooperation between the content owners and various stakeholders such as Distribution Companies, Device Manufacturers, and Multichannel Video Programming Distributor (MVPD) Partners.

A. Digital Watermarks Can Block Content Available on Televisions

In the broadcast television scenario, when a device such as a set-top box or a newer television with expanded capabilities is enabled to read the watermark, it can allow parents to set parameters of content accessibility: Block all "Mature Audience" content and/or "look up sub-rating of designated 'Mature Audience' and block 'TV-14' and higher designations.

B. Digital Watermarks Can Block Content Available Through Cable and Satellite Transmission

In the cable or satellite transmission scenario, as with broadcast television, when a device, such as a set-top box or a newer television with expanded capabilities, is enabled to read the watermark it can allow parents to set parameters of content accessibility: Block all "Mature Audience" content and/or "look up sub-rating of designated 'Mature Audience' and block 'TV-14' and higher designations.

C. Digital Watermarks Can Block Content Available on Wireless Devices

When a mobile device is enabled to read the watermark it can allow parents to set parameters of content accessibility: Block all "Mature Audience" content and/or "look up sub-rating of designated 'Mature Audience' and block 'TV-14' and higher designations.

D. Digital Watermarks Can Block Content Available on Non-Networked Devices

When a non-networked device, such as a DVD player, is enabled to read the watermark it can allow parents to set parameters of content accessibility: Block all "Mature Audience" content. In this case, additional rating information might be pre-programmed into the device itself, allowing further blocking based on the sub-rating of designated 'Mature Audience' content.

E. Digital Watermarks Can Block Content Available Over the Internet

As discussed above, digital watermarks can be designed to carry both semantic information and a reference number. The information carried by the watermark can include the highest level "label" (e.g. "Mature Audience") mandated by a regulatory ratings body or a voluntarily rating agreed to by industry participants. The reference

number points to an online database in which the "connected" device can further classify the content based on distribution channel (e.g. The Entertainment Software Rating Board (ESRB) ratings that are designed to provide concise and impartial information about the content in computer and video games so consumers, especially parents, can make an informed purchase decision; or the Family Online Safety Institute's Internet Content Rating system). When a device such as a PC or laptop is enabled to read the watermark, it can allow parents to set parameters of content accessibility: Block all "Mature Audience" content and/or "look up sub-rating of designated 'Mature Audience' and block 'T' (Teen Rated) and higher designations.

IV. Digital Watermarking Is An Available and Effective Parental Empowerment Tool

As part of the FCC's inquiry on other available advanced blocking technologies, it is important to consider the basic characteristics of the technology to be adopted and deployed.[2] Digimarc believes, based on our broad experience and those of our partners and licensees in developing mass market systems, at least five characteristics are critical to a successful deployment.[3] These characteristics include: scalability, content agnostic, format independence, maturity, and extensibility.

- **Scalability:** The technology must be able to work with a wide variety of content types (from music and images to games and video) and devices including personal content consumption devices such as portable media players, and should be broadly deployable.

- **Content Agnostic**: The technology should be applicable to all forms of content, including those referenced by the NOI (i.e., images, audio, and video content).

- **Format Independence**: The technology must not rely on a particular common content format such as a standard DVD format, Digital Broadcast format or

[2] Fostering broad adoption of advanced blocking technologies will require government and industry leadership, orchestration of all the stakeholders, and an underlying recognition that consumer value is paramount. Where there is consumer value, there is incentive within industry to innovate and offer solutions. Since the market for parental control to date has not been of sufficient size to stimulate broad-based innovation or deployment, government and industry should pursue orchestrated industry approaches wherein parental controls are a component of a full set of features that offer commercial value.

[3] As is common with industry initiatives where broad-based adoption is the goal, success rides on the openness and collaboration of the standards-setting process, a level playing field for all in the ecosystem, and the ability for implementers to derive value through their own differentiation and add-on applications. This ultimately leads to a self-sustaining marketplace in which industry is motivated and incentivized to invest.

Theatrical Release format. It must remain independent of a particular type of content format so that it is not limited in its utility and future applications.

- **Maturity**: The technology should be adopted and used by industry partners. Technologies that are in use and relied upon for "mission-critical" applications have a substantially greater chance of adoption for add-on purposes than those that are brand new or unproven.

- **Extensibility:** The technology must be compatible with other devices. Consumers demand that content is interoperable while expecting new functionality and utility during each device upgrade and adoption cycle.

Digital watermarking embraces all of the above characteristics.[4] It is content agnostic, extensible, and device and format independent. And, as mentioned above, private industry has already adopted digital watermarking technology for multiple applications. Specific instances of such deployments are set forth in the appendices to this comment letter. [5]

Used as an advanced blocking technology, digital watermarks can offer multiple benefits to parents who wish to regulate their children's media and entertainment access. Digital watermarking can:

- Enable parents to block content based on highly specific personal preferences;

[4] Digital watermarking exhibits all the traits required for a successful parental control solution. It is content agnostic (images, video, and audio), device independent (integrated in devices and networks) and format independent, surviving through digital and analog transformations. Content ratings information can and is currently carried by digital watermarks for multiple applications and can be augmented by additional services provided by industry partners to serve parental control needs. Consistent, industry-wide application of digital watermarking to content, regardless of format, can offer multiple benefits to parents who wish to regulate their children's access.

[5] Attached to this comment letter and incorporated herein are a series of appendices that provide examples of the wide deployment of digital watermarking within various ecosystems. These include:

- Appendix A: Current Applications of Digital Watermarking
- Appendix B: Digital Watermarking in the Television and Movie Industry
- Appendix C: Digital Watermarking in the Music Industry

We have also included information regarding a U.S. Supreme Court case to which Digimarc contributed an amicus brief, and insights as to certain standards and components of parental filtering solutions:

- Appendix D: Components of a Parental Filtering Solution
- Appendix E: The US Supreme Court Recognition of Digital Watermarking

- Allow for more appropriate targeting of advertising or related content for kids versus adults;

- Disallow uploading of inappropriate content onto social media sites for kids;

- Make Internet searching safer by filtering results; and

- Determine whether content is appropriate for viewing based on the originating country's cultural norms.

In sections III and IV, we have discussed the ease with which parents could utilize the technology. Appendices A through D give specific examples of how the technology is currently deployed in various ecosystems, and the breadth with which the technology has been deployed.

V. Digital Watermarking Technology Offers Incentives For Parents and Content-Providers, Which Will Encourage Its Development, Deployment, and Use

The FCC's NOI also sought comment on the methods of encouraging the development, deployment, and use of advanced blocking technologies. Digimarc submits that unlike previous blocking technologies that found little support outside of the home, both private industry and consumers will support and encourage the deployment and use of digital watermarking technology.

Private industry has already supported the development and use of digital watermarks to protect and monitor its work. Industry is deploying watermarking as an effective forensic tracking tool, successful in detecting and deterring digital counterfeiting and piracy. Because media content is already being watermarked, additional information can be inserted during production or distribution to assist in child protection.

The music industry, for example, has been using digital watermarking for more than six years to curtail pre-release piracy. In this case, the industry has applied digital watermarks to advance copies of CDs that identify individual copies of the same CD. Thus, when a sound track is leaked, the identity of the source is known. This has proven effective to deter leakage and piracy of pre-release music.

Recently the Recording Industry Association of America ("RIAA") developed a common specification that defines a specific watermark format as a technical standard for all music. This specification will enable a common watermark for identifying music online as well as enabling Parental Advisory information. For more information, please see: http://www.riaa.com/whatwedo.php?content_selector=technical_standards. See also Appendix C for additional information regarding use in the music industry.

As the FCC undertakes an examination of advanced blocking technologies that can operate across multiple platforms, it is worth noting that the digital world complicates implementing controls envisioned by the Child Safe Viewing Act. It is important to

remember that content becomes "anonymous" when it is made digital – the content is just one or more digital files.[6] Thus the content owners and their distribution partners need persistent identifiers to be able to identify, manage, and monetize their content.[7] These same identifiers are exactly what parents need, in order to monitor and protect their children from objectionable content in a digital world. Accordingly, there is a confluence of interest between parents and private industry in the need for a persistent content identifier, even though they will use the technology for different purposes. And because watermarking is "imperceptible," with respect to the enjoyment of the content, it will be "transparent" and "inaudible" to the consumers of that content.

VI. Digital Watermarking Technology Is More Functional and Portable Than the V-Chip and Therefore Will Be Adopted Faster Than V-Chip Technology

The FCC also requested comment in the NOI on how to improve V-Chip technology. We believe that the problem with current parental control solutions, such as the V-Chip, is that they were explicitly designed for specific channels of distribution that did not contemplate portability to other channels or devices. This results in functionality that is constrained by the device (e.g., the television) or by the application on which it runs (e.g., TiVO applications), and cannot be readily expanded to include other media platforms, media types and content formats. As more and more content is distributed through multimedia platforms, parents will be less likely to invest in technology that blocks content from only one distribution point, such as a television. Children would likely be able to get the objectionable content from other distribution sources that are not supported by the blocking technology. The heterogeneity of distribution demands a content-persistent solution, not one that is device, channel or distribution method specific.

Digital watermarking addresses this issue and gives parents the ability to block content on multiple devices. As such, parents will be more likely to invest the time to understand and adopt digital watermarking technology since it can be used to block any indecent or objectionable programming regardless of platform.

---

[6] When content is digitized it is turned into generic and non-descript computer files. A "movie" is now just a Windows Media File, an Adobe Flash file or an MPEG4 file with whatever name the user assigns it. A song is now just an MP3 file with whatever name a user gives it. And an image is now just a JPEG file with whatever name a user gives it. Thus, digitization has the side effect of "anonymizing" content.

[7] As content and content distribution increasingly goes digital, private industry has invested hundreds of millions into R&D to find ways to persistently and accurately identify content in its digital form, including ways to attach persistent identities to movies, music, and images – identities that survive copying and editing, transformations from analog to digital and back, and any number of format changes. These identities are critical to conveying copyright ownership, tracking usage, and allowing or blocking access as digital distribution paths multiply and evolve and devices proliferate.

Conclusion

In summary, Digimarc respectfully submits that digital watermarking is one of the *very few technologies, if not the only technology*, available that is capable of operating across multiple content types and multiple platforms while addressing all of the FCC requirements for achieving effective content blocking. Digimarc further asserts that the FCC's investigation focuses on enabling the content itself to be a permanent, intrinsic and declarative part of the advanced blocking solution in any and all distribution channels, both present and future.

Digital watermarks are *content-persistent*, rather than channel or device-specific and can inherently become part of an advanced content blocking solution.

Digimarc would like the opportunity to meet with Commission Staff to demonstrate digital watermarking as a technology that is (1) compatible with various communications devices and platforms; and (2) can improve and enhance the ability of parents to protect their child from any indecent or objectionable audio or video programming, transmitted through the use of wire, wireless, or radio communications.

Digimarc appreciates the FCC's work on the Child Safe Viewing Act and the Examination of Parental Control Technologies for Video or Audio Programming. We look forward to continuing to assist and advise the FCC in this important undertaking and are committed to protecting children as we move into an increasingly interconnected and interoperable society.

Respectfully submitted,

Robert P. Chamness
EVP, CLO, and Secretary
Digimarc Corporation

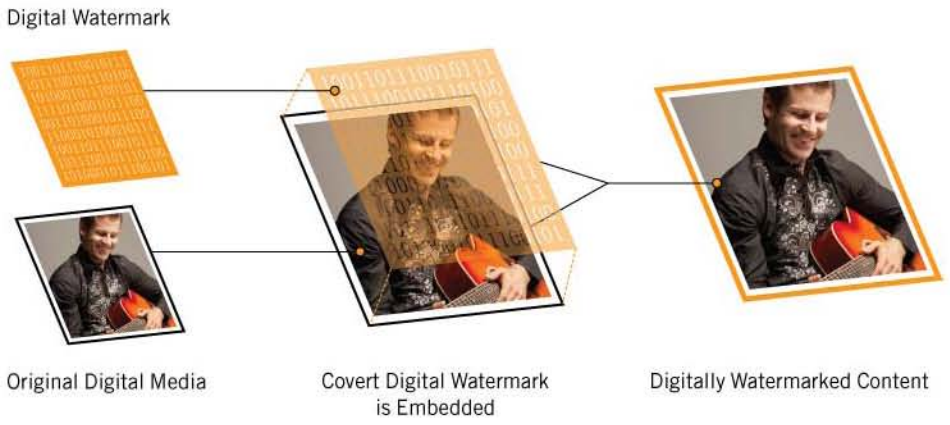
Appendices attached:

- Appendix A: Current Applications of Digital Watermarking
- Appendix B: Digital Watermarking in the Television and Movie Industry
- Appendix C: Digital Watermarking in the Music Industry
- Appendix D: Components of a Parental Filtering Solution
- Appendix E: The US Supreme Court Recognition of Digital Watermarking

Appendix A: Current Applications of Digital Watermarking

Digital watermarks have been broadly and successfully deployed across a number of highly useful applications.

Figure 1



Broadcast Monitoring: Broadcast monitoring allows interested parties to know where, when and how certain pieces of content are being aired. Every day, thousands of programs and advertisements run in thousands of markets around the world. With highly regionalized cable, satellite and terrestrial delivery, advertisers need to know that the ads they're paying for are actually being broadcast. Networks need to know where their programming is running.

Advertisers such as Coca Cola and Pepsi, and networks such as ABC Television Network, NBC News Channel, BBC and Reuters Television, rely on broadcast monitoring services to routinely look for watermarks in programming on hundreds of channels worldwide. This monitoring is offered by companies such as Civolution, Verance, and Nielsen Media Research. In fact, Teletrax broadcast monitoring solutions cover more than 800 television stations and cable channels in the U.S. alone, accounting for more than 85% of all television households. Broadcast monitoring using digital watermarking allows networks to evaluate the reach of their programming, and advertisers to measure the effectiveness of their campaigns.

Copy Prevention: Digital watermarks allow companies to control the use of copyrighted image, audio and video content. A digital watermark travels with the content, persisting through the changes in file format, through encryption and decryption, and through transformation between digital and analog form. This allows the content owner to specify whether or how often the work can be legally copied or shared without visually or audibly impairing the work. It also allows greater and safer dissemination of copyrighted works while at the same time ensuring appropriate compensation to the owners.

Recent reports highlight the fact that utilities now exist to bypass most encryption-based copy protection safeguards for music, except for digital watermarks. That is why audio watermarking, provided by Digimarc business partner, Verance Corporation, is an integral component of a successful industry standard playback and record control system for a consortium consisting of Intel, IBM, Matsushita (Panasonic), and Toshiba, known as the 4C Entity. As a result, when copyrighted audio content is illegally copied to a new disc and played on a device built to the new standard, the device will halt playback.

Forensic Tracking: Forensic tracking allows content owners to determine when and where a piece of content leaves its authorized distribution path. The most common use of forensic tracking is in the entertainment industry, where music and movies are routinely distributed to executives, critics and other media outlets for promotion before they're released to the public. In recent years, copies of these 'pre-release' products have been leaked onto the Internet, copied onto CDs and DVDs, and sold as "bootlegs" well ahead of their commercial releases. This can result in a loss of revenue for the artists, the studios and the music labels.

To combat pre-release piracy, music companies and movie studios embed pre-release content with digital watermarks that are unique to each authorized recipient. This allows the content creators to forensically track the source of the leak and take appropriate action. As a result, recipients of pre-release music and movies have begun to police themselves because they know that leaking these materials will result in certain personal liability.

Civolution, Thomson, Media Science International, Verance, Verimatrix, MarkAny, and Digimarc are supplying audio watermarking solutions designed to deter piracy of pre-release audio content. Currently, digital watermarking is incorporated in millions of audio tracks from the major record labels to identify and track leaks of promotional pre-release music onto the Internet. Major record labels such as SonyBMG, Universal Music Group, Warner Music, mastering studios, disc duplicators and online business-to-business music distributors are customers of digital watermarking solutions from Digimarc Business partners.

Rights Management: Because digital watermarks can be applied and detected at virtually every point between distribution and playback, they become invaluable for rights management and re-association. This means that consumers can move their digitally watermarked content through their various playback devices (e.g. personal computers and CD players) and environments without losing their rights to that content and ensuring playability.

Rights management with digital watermarking also has the potential to change the landscape of peer-to-peer (P2P) networks. For instance, if a P2P network were to incorporate digital watermarking software in its client application, it would help facilitate legal file sharing, and ensure that consumers have appropriate access to legitimate content. The Distributed Computing Industry Association, a trade

organization representing peer-to-peer software providers, content rights holders, and service-and-support companies, advocates the use of digital watermarking for the protection of entertainment content authorized for P2P distribution.

Remote Triggering: Digital watermarking can be used as a trigger—to make a playback device, like a cell phone or a digital video recorder, perform an automatic action. When images, audio or video files are distributed or received, digital watermarks can signal these devices to trip a download counter or display additional related content and choices to consumers.

Filtering/Classification: The popularity of Napster, a free peer-to-peer (P2P) music swapping service, brought the issue of content management to a crisis point. Because P2P systems have difficulty determining which audio files are copyrighted and which are not, it is relatively easy for content to be illegally distributed across these networks. Digital watermarks allow P2P systems to easily identify and distinguish copyrighted from non-copyrighted audio or video files. Digital watermarks can even enhance P2P systems by enabling them to collaborate with record labels and other audio retailers to market legitimate copyrighted songs.

This issue was highlighted in the recent U.S. Supreme Court ruling against P2P network Grokster. In its opinion, the Court specifically identified digital watermarking as one of the technologies that could be used to deter illegal file sharing. (more detail in section, below) The digital watermarking technology that helps to maintain the integrity of copyrights also empowers consumers to take further and deeper control of digital content. Digital watermarking can be used to sort and search through audio, image and video files. For example, digital images could be embedded with digital watermarks that allow devices to classify or filter them in order to help parents better manage the media intake of their children.

E-Commerce: Digital watermarking can be used to further enhance the consumer experience through improved electronic- and mobile-commerce applications. Once entertainment content or printed material is identifiable in any format through a digital watermark, consumers have numerous options available to them. For example, when a digitally watermarked song is heard by a consumer with a watermark-aware cell phone, a content ID can be used to download legitimate copies of the artist's music. The same technology could enable the consumer to get local concert information, read reviews, and even purchase tickets directly through their cell phone. These applications have the potential to give consumers more choices, better access and faster delivery of the products and entertainment they want.

Counterfeit Deterrence: Digital watermarking has been employed by national governments and a consortium of central banks globally to deter the counterfeiting of currency.

Appendix B: Digital Watermarking in the Television and Movie Industry

In the television and movie industry, applications of digital watermarking range from pre-release anti-piracy and theatrical release piracy deterrence through to broadcast verification and audience measurement. In each of these diverse application areas, the technology has already been integrated into both existing and traditional workflows as well as new and emerging digital workflows. In some cases, such as Digital Cinema (the general move to use digital technology to distribute and project motion pictures versus film reels), digital watermarking has been mandated as part of the movie industry's security standards and will ultimately be integrated into all Digital Cinema servers worldwide over the next five years.

The television and movie industry is serviced by a variety of digital watermarking technology, solutions, and service providers. These include:

Nielsen: The Nielsen Company is best known for The Nielsen Ratings—the market intelligence/television ratings system that fundamentally helps set the advertising rates on television. Nielsen uses digital watermarking to automate the ratings process as well as to authenticate broadcasts. Nielsen is currently working with Digimarc to develop a core content identification solution to address non-linear distribution of content on the Internet.

Verance: Verance offers copy management solutions for film, video, and music. Verance's Cinavia technology has been selected for use within the AACS (security standard for next generation of optical discs and DVDs) security standard to enable the communication and enactment of use policies for audiovisual content across a broad range of distribution channels and devices.

Thomson: Thomson provides its clients with several content tracking and security solutions as part of its digital watermarking-based NexGuard™ and NexTracker™ product lines.

Civolution: Civolution offers audio and video watermarking solutions. Civolution was formed in October 2008 as a spin-out of Royal Philips Electronics and is a world leading technology and services provider for identifying, managing and monetizing media content. Civolution offers cutting-edge digital watermarking technology solutions for forensic tracking of media assets in pre-release, digital cinema, payTV and online.

Appendix C: Digital Watermarking in the Music Industry

One of the applications being considered for implementation by the music industry, in collaboration with technology and solution partners, is the embedding of a Parental Advisory watermark that could be offered to consumers in an effort to help concerned parents protect young children from exposure to explicit musical content.

Unlike other segments of the entertainment industry, the recording industry does not have a formal regulatory infrastructure for the mandated inclusion of parental content rating information. No committees, boards, or commissions review musical or lyrical content. Although FCC restrictions can impact what gets broadcast on the radio, no meaningful restrictions—self-imposed or otherwise—exist on what gets produced and shipped to the public. Instead, music labels attach a simple "Parental Advisory: Explicit Content" sticker to anything they that may be construed as objectionable material. In general this is a very discretionary process and is completely voluntary and only supported by the major member music labels which comprise the membership of the Recording Industry Association of America (RIAA).

Although independent record labels and music retailers are under no obligation to offer this labeling, some music retailers, including iTunes, also provide a label in the digital storefront characterizing explicit music as such, and in some cases, offer a "clean" version right next to the explicit version as an alternative. However, there is no mechanism to prevent a young child from listening to or even acquiring the music short of parental oversight – a task made difficult by the generally private manner in which digital music is consumed with headphones or earbuds.

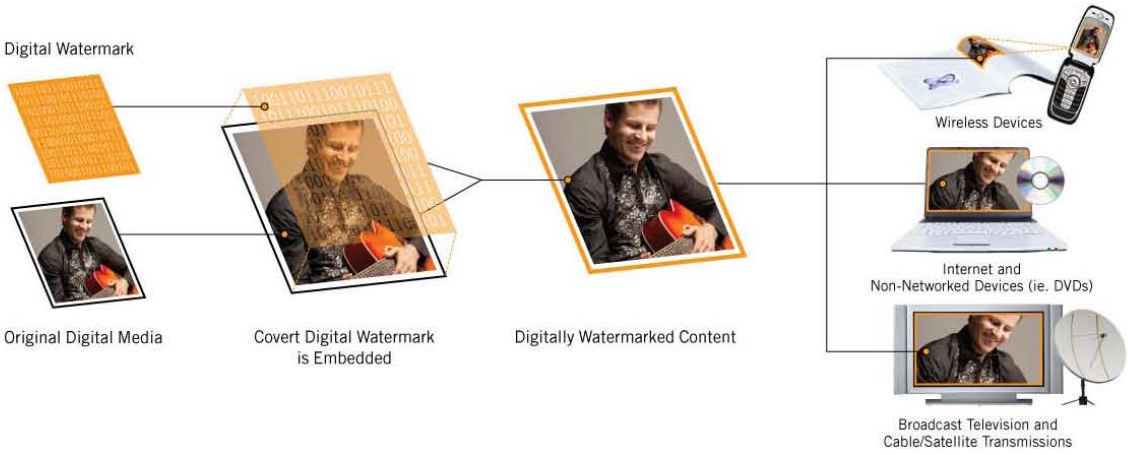
Appendix D: Components of a Parental Filtering Solution

A parental filtering solution is comprised of three functional blocks; Classification, Labeling and Action. All three can occur anywhere prior or during the play-out of content (audio, video, still imagery) for consumption by children. The earlier the functional blocks can occur in the content creation, distribution and play-out process, the more efficiencies for the system and more impactful the result.

Utilizing broadcast television destined for linear distribution (a television network distributing content through affiliate stations) can have the Classification and Labeling step occur at the content creation step. During post production, content can be classified and labeled as such, surviving transmission through the affiliate station for ultimate action to be taken at the playing device.

Performing these steps earlier in the process and labeling the content in a persistent fashion ensures that regardless how the content is re-purposed in the future, through syndication, distribution via non-linear sites (Hulu, etc.), etc., the parental filtering action is still enabled.

Figure 2



It should be noted that this does not preclude additional classification and labeling from occurring during the distribution process. For example, as a value added service by a distributor that better understands the needs/desires of its audience, additional or deeper classification might occur by the television affiliate in the linear distribution model or by the website supporting non-linear distribution, etc.

Action can occur at any step after labeling, but may happen early in the distribution channel (programming), later in the distribution channel (filtering), or at the player. Examples of each follow.

Action in the form of pre-meditated collection and filtering of content can and is currently done, resulting in kid-safe linear broadcast channels and internet sites. This is

accomplished by the traditional role of the programmer. This results in “walled-gardens” where content is presumably not of concern. As content is sourced from disparate sources, these walled-gardens are difficult to support and ultimately rely on automated filtering mechanisms from vendors such as Rule-Space and others. The natural conclusion of this arc is the deployment of classification and filtering solutions at the content consumption device, utilizing tools such as Net Nanny and others for IT devices. Classification, however, is an expensive and intricate process and is ideally suited for personal computers, not consumer or mobile devices.

Opportunities to take action are being leveraged at other locations in the distribution channel, particularly for non-linear models, such as at the ISP, home media server or P2P client. This creates new opportunities to aggregate traffic destined for children and possibly take action.

The Classification and Action functional steps both present opportunities for industry partners to add value and provide services in support of the desired goal of better parental control.

Classification is currently done by manual or automated means; however, it is at the parents’ discretion as to what the appropriate action should be for a particular class of content. Parents can rely on self-classification by content owners and distributors, similar to the V-Chip implementation or may choose to leverage additional services to augment the granularity of the classification. Utilizing the prior example, parents may select distribution channels that put a premium on high granularity classification of content, or might utilize filtering tools themselves at a media server in the home to provide another level of detail.

Action can be driven by a set of rules at the discretion of the parent similar to V-Chip, but can be extended providing more control. The movie industry currently uses a set of rules to communicate rules and control distribution of content in non-linear channels that are well understood. Leveraging such models, and with the provision of a simplified ‘control panel,’ parents can determine when and what actions should be taken against labeled content.

Appendix E: U.S. Supreme Court Recognition of Digital Watermarking

Everyone agrees that consumers deserve to have access to the entertainment options available to them. Likewise, content owners and artists deserve to be recognized and compensated for their work. However, policymakers and courts have often been asked to choose sides because of the difficulties associated with how to protect these rights.

The U.S. Supreme Court has recognized the capacity of digital watermarking to create win-win solutions in the face of tough policy issues. When the rapid proliferation of file sharing networks (also known as peer-to-peer or P2P networks) enabled users to illegally exchange copyrighted material such as digitized movies and music, the Court was asked to address the question of liability in the case in Metro-Goldwyn-Mayer Studios v. Grokster.

The Court ruled that file sharing networks can be held liable when their users illegally exchange copyrighted material, in part because of readily available technologies like digital watermarking that can be used by rights holders and file sharing networks to deter piracy and illegal use of copyrighted entertainment content.

As a direct result of the Court's decision, the Distributed Computing Industry Association (DCIA), a trade organization representing peer-to-peer software providers, content rights holders, and service-and-support companies, announced a resolution to support digital watermarking for the protection of entertainment content authorized for P2P distribution:

> "Through our discussions, we concur with the Supreme Court that digital watermarking – which has already gained strong adoption by the content community in the business-to-business (B2B) segment of the distribution chain – offers meaningful resolution to the issue at hand."
> …
> "The DCIA believes that this technology, which is available from multiple vendors worldwide, is not only a natural solution for content providers, but one that we as an industry should embrace. We therefore reach out to our content partners in light of the Grokster decision, and invite them to adopt this technology and embed watermarks that identify content, state, and/or specific allowable uses.
> …
> "As the content community has already begun adoption and realized success with digital watermarking technology, we further believe that the extension of their current use of the technology within the P2P marketplace should be deemed cost-efficient and a no-lose proposition.
>
> "Furthermore, we believe that by incorporating watermark detection in P2P clients and systems, the P2P community will truly establish a collaborative and mutually profitable environment for all parties."
>
> – DCIA letter to content and technology industry Jan 11 06